(19)日本国特許庁(JP)

(12)公開特許公報（A）

(11)特許出願公開番号

特開平１１－６５４４３

(43)公開日　平成11年(1999)3月5日

(51)Int. Cl.[6]		識別記号	FI		
G09C	1/00	640	G09C	1/00	640 E
		630			630 D
G06F	19/00		G06F	15/30	Z
H04L	9/32				340
			H04L	9/00	675 D

審査請求　未請求　請求項の数１４　ＯＬ　（全７頁）

(21)出願番号　特願平９－２１９３９８

(22)出願日　平成9年(1997)8月14日

(71)出願人　000102728
株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目3番3号

(72)発明者　服部　昇
東京都江東区豊洲三丁目3番3号　エヌ・ティ・ティ・データ通信株式会社内

(72)発明者　奈須　善幸
東京都江東区豊洲三丁目3番3号　エヌ・ティ・ティ・データ通信株式会社内

(72)発明者　坂田　祐司
東京都江東区豊洲三丁目3番3号　エヌ・ティ・ティ・データ通信株式会社内

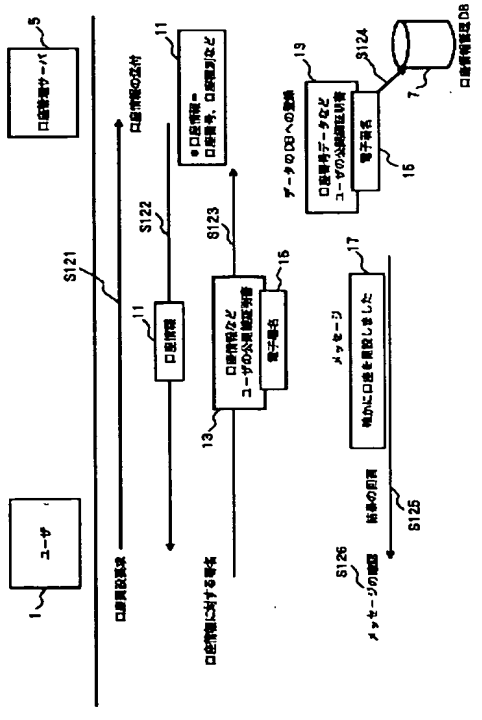
(74)代理人　弁理士　上村　輝之

(54)【発明の名称】個人認証情報の管理方式

(57)【要約】

【課題】　個人認証情報の第三者による不正使用や改竄を防止すると共に、個人情報の管理機関が必要に応じて内容を確認できるようにする。

【解決手段】　ユーザ１は口座管理サーバ５に口座種別等を明示した口座開設要求を送付する。口座管理サーバ５は口座の新規開設に伴う口座情報１１をユーザ１に送付する。ユーザ１は口座情報１１の内容を確認してＣＡからの公開鍵証明書を結合させ自己の個人認証情報１３を生成する。個人認証情報１３に対し、公開鍵証明書の公開鍵に対応する個人秘密鍵により電子署名１５を作成する。電子署名付き個人認証情報１３を口座管理サーバ５に送付する。口座管理サーバ５は、個人認証情報１３内の公開鍵証明書を用いて電子署名１５の検証を行い、個人認証情報１３の正当性を確認する。個人認証情報１３を電子署名１５を添付した状態で口座情報管理ＤＢ７に登録する。口座管理サーバ５は新規口座開設の確立のメッセージ１７をユーザ１に送付し、ユーザ１がメッセージ１７を確認すると口座開設要求に関する一連の処理動作が完了する。



1

【特許請求の範囲】

【請求項１】　ユーザと情報管理機関との間で授受される個人認証情報の管理方式において、

前記ユーザ固有のコード情報と前記ユーザの公開鍵情報とから構成される個人認証情報を生成する生成手段を備えることを特徴とする個人認証情報の管理方式。

【請求項２】　請求項１記載の個人認証情報の管理方式において、

前記生成手段が、前記ユーザに備えられることを特徴とする個人認証情報の管理方式。

【請求項３】　請求項１記載の個人認証情報の管理方式において、

前記個人認証情報が、前記ユーザと前記情報管理機関が備えるサーバとの間で授受されることを特徴とする個人認証情報の管理方式。

【請求項４】　請求項１記載の個人認証情報の管理方式において、

前記個人認証情報が、前記ユーザと前記サーバとの間で行われる取引において授受されることを特徴とする個人認証情報の管理方式。

【請求項５】　請求項４記載の個人認証情報の管理方式において、

前記取引が、前記ユーザと前記サーバとの間で行われるオンラインでの商取引であることを特徴とする個人認証情報の管理方式。

【請求項６】　請求項１記載の個人認証情報の管理方式において、

前記情報管理機関が、金融機関であり、

前記コード情報が、前記金融機関において開設されるユーザの口座を示す番号情報であることを特徴とする個人認証情報の管理方式。

【請求項７】　請求項１記載の個人認証情報の管理方式において、

前記公開鍵情報が、予め第三者機関である認証局からユーザ自身の個人認証情報として使用するために取得されたものであることを特徴とする個人認証情報の管理方式。

【請求項８】　請求項７記載の個人認証情報の管理方式において、

前記公開鍵情報に対応する個人秘密鍵情報を更に有することを特徴とする個人認証情報の管理方式。

【請求項９】　請求項８記載の個人認証情報の管理方式において、

前記個人秘密鍵情報が、前記ユーザにおける個人認証情報に添付する電子署名の作成に用いられることを特徴とする個人認証情報の管理方式。

【請求項１０】　請求項１乃至請求項９のいずれか１項記載の個人認証情報の管理方式において、

前記ユーザが、

前記サーバに対し、口座の開設要求を送付するための第

2

１の手段と、

前記サーバに対し、開設されている口座に関する指示メッセージを送付するための第２の手段と、

前記開設要求又は前記指示メッセージが送付されたとき、前記作成された電子署名付きの個人認証情報を前記サーバに送付するための第３の手段と、

を更に備えることを特徴とする個人認証情報の管理方式。

【請求項１１】　請求項３乃至請求項１０のいずれか１項記載の個人認証情報の管理方式において、

前記サーバが、前記第３の手段により送付された個人認証情報に含まれる公開鍵情報を使用して前記添付された電子署名を検証することにより、前記電子署名付き個人認証情報の正当性を検証する検証手段を備えることを特徴とする個人認証情報の管理方式。

【請求項１２】　請求項１１記載の個人認証情報の管理方式において、前記情報管理機関が、前記検証手段によって正当性を検証された前記電子署名付き個人認証情報を登録するための記憶手段を備えることを特徴とする個人認証情報の管理方式。

【請求項１３】　請求項３乃至請求項１２のいずれか１項記載の個人認証情報の管理方式において、

前記サーバが、

前記登録されている個人認証情報に含まれる公開鍵情報により、前記第２の手段により送付された指示メッセージの正当性を検証する検証手段と、

前記指示メッセージの正当性が確認されたとき、その指示内容を実行する実行手段と、

を更に備えることを特徴とする個人認証情報の管理方式。

【請求項１４】　請求項１３記載の個人認証情報の管理方式において、

前記検証手段が、前記登録されている電子署名付きの個人認証情報に基づき、前記ユーザから与えられる指示メッセージが口座開設者自身からの指示であるか否か、及び第三者により指示内容が改竄されているか否かを確認することにより前記指示メッセージの正当性を検証することを特徴とする個人認証情報の管理方式。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ユーザと個人情報を管理する管理機関のサーバとの間で授受される個人認証情報の管理方式の改良に関するものである。

【０００２】

【従来の技術】従来、金融機関（銀行）と口座開設者（個人又は企業）との間のオンラインや他の形態での取引において、金融機関が取引当事者を口座開設者か否か確認するための手段として、口座開設者の個人認証情報を利用する方法が実施されている。個人認証情報には、予め口座開設者が選定した暗証番号が用いられ、暗証番

号は、金融機関の下で漏洩や不正な改竄が行われないよう管理されている。

【０００３】

【発明が解決しようとする課題】ところで、暗証番号は上述したように、一般にＰＩＮ（パーソナル・アイデンティフィケーション・ナンバー）として利用されるものであるが、個人認証情報の中でも第三者にとって利用可能なものの一つである。そのため、上記ＰＩＮが漏洩した場合には、そのＰＩＮに対応する個人（又は企業の）口座が第三者から不正アクセスされる虞が生じる。また、上記ＰＩＮ等の個人認証情報は、それを管理する金融機関においてさえも、不正に変更（改竄）される虞が全くないとは言い難い状況にある。

【０００４】このように、個人認証情報が置かれている状況は、セキュリティ面で必ずしも満足のいくものではない。しかし、セキュリティ面ばかりを考慮して個人認証情報を本人以外には全く解読できないようにすれば、仮に口座開設者（個人又は企業）から金融機関に対し何らかの取引上の要求があってその要求の正当性を確認する必要が生じたときに、金融機関が自由に口座開設者の個人認証情報を利用できなくなるという問題が生じてしまう。このように、従来にあっては、個人認証情報のセキュリティを向上させようとすれば、個人認証情報の管理機関である金融機関が自由にその個人認証情報を利用できなくなるという問題があった。

【０００５】従って本発明の目的は、個人認証情報の漏洩が生じても第三者に利用されたり内容が改竄されたりする虞がなく、且つ、個人情報の管理機関が必要に応じて内容を確認することが可能な個人認証情報の管理方式を提供することにある。

【０００６】

【課題を解決するための手段】本発明に従う個人認証情報の管理方式は、ユーザと情報管理機関との間で授受される個人認証情報の管理に関するもので、ユーザ固有のコード情報とユーザの公開鍵情報とから構成される個人認証情報を生成する生成手段を備える。

【０００７】本発明に係る好適な実施形態では、生成手段は、ユーザに備えられている。そして、個人認証情報は、ユーザと情報管理機関が備えるサーバとの間で授受されるもので、例えば、ユーザとサーバとの間で行われる取引において授受されるものである。上述した取引としては、例えば、ユーザとサーバとの間で行われるオンラインでの商取引がある。

【０００８】情報管理機関とは、銀行等の金融機関のことであり、ユーザ固有のコード情報とは、金融機関において開設されるユーザの口座を示す番号情報のことである。

【０００９】上述した公開鍵情報は、予め第三者機関である認証局（ＣＡ、即ち、サーティフィケーション・オーソリティの日本語訳）からユーザ自身の個人認証情報として使用するために取得されたものである。上記個人認証情報は、この公開鍵情報に対応する個人秘密鍵情報を更に有している。この個人秘密鍵情報は、ユーザにおける個人認証情報に添付する電子署名の作成に用いられるものである。

【００１０】この電子署名の添付により、第三者によるユーザの口座への不正アクセスが防止でき、また、情報管理機関におけるユーザの個人認証情報の変更（改竄）が防止できる。

【００１１】上記実施形態では、ユーザは、上述した生成手段に加えて、サーバに対し口座の開設要求を送付するための第１の手段と、サーバに対し開設されている口座に関する指示メッセージを送付するための第２の手段と、開設要求又は指示メッセージが送付されたとき作成された電子署名付きの個人認証情報をサーバに送付するための第３の手段とを更に備えている。

【００１２】一方、サーバは、上記第３の手段により送付された個人認証情報に含まれる公開鍵情報を使用して添付された電子署名を検証することにより、電子署名付き個人認証情報の正当性を検証する検証手段を備えている。この検証手段によって正当性を検証された電子署名付き個人認証情報は、情報管理機関が備える記憶手段に登録される。サーバは、上記第１～第３の各手段に加えて、登録されている個人認証情報に含まれる公開鍵情報により、第２の手段により送付された指示メッセージの正当性を検証する検証手段と、指示メッセージの正当性が確認されたとき、その指示内容を実行する実行手段とを更に備えている。

【００１３】指示メッセージの正当性を検証する検証手段は、登録されている電子署名付きの個人認証情報に基づき、ユーザから与えられる指示メッセージが口座開設者自身からの指示であるか否か、及び第三者により指示内容が改竄されているか否かを確認することにより指示メッセージの正当性を検証する。

【００１４】上記検証手段によって、情報管理機関は必要に応じて口座開設者の個人認証情報を利用することが可能になる。

【００１５】

【発明の実施の形態】以下、本発明の実施の形態を、図面により詳細に説明する。

【００１６】図１は、本発明の個人情報の管理方式が適用されるオンライン金融取引システムの一実施形態を示すブロック図である。

【００１７】上記システムは、ユーザ側の端末（ユーザ）１と、銀行に代表される口座管理機関３側のサーバ（口座管理サーバ）５及び口座情報管理ＤＢ（口座情報管理データベース）７とを備えており、ユーザ１と口座管理サーバ５とがネットワーク９を介して接続されて構成される。上記システムでは、ユーザ１が予め信頼できるＣＡ（図示しない）から個人認証情報として使用する

自己の公開鍵についての証明書（公開鍵証明書）を取得しておくことが、以下に実行される処理動作の前提になる。なお、その公開鍵証明書によって証明されている公開鍵に対応するユーザ１の個人秘密鍵は、例えばＩＣカード（図示しない）等に秘密に保管されるものとする。

【００１８】ユーザ１は、口座管理機関３（口座管理サーバ５）に対する口座開設要求の送付や、口座サーバ５から送付される口座番号情報及び口座種別情報等の口座情報と上記公開鍵証明書との結合による個人認証情報の生成や、上記公開鍵に対応する個人秘密鍵により作成した電子署名の個人認証情報への添付を行う。ユーザ１は、また、電子署名付き個人認証情報の口座管理サーバ５への送付や、口座管理サーバ５から送付される新規口座開設が確立された旨のメッセージの確認をも行う。ユーザ１は、更に、自己の口座に関する指示要求メッセージの口座管理サーバ５への送付や、上述した態様で作成した電子署名の指示要求メッセージへの添付や、電子署名付き指示要求メッセージの口座管理サーバ５への送付や、口座管理サーバ５から送付される処理完了メッセージの確認をも行う。

【００１９】口座管理サーバ５は、口座の新規開設に伴う口座情報のユーザ１への送付や、上記公開鍵証明書を用いた電子署名の検証によるユーザ１の個人認証情報の正当性の確認や、電子署名付き個人認証情報の口座情報管理ＤＢ７への登録を行う。口座管理サーバ５は、また、新規口座開設が確立された旨のメッセージのユーザ１への送付や、口座情報管理ＤＢ７に登録済みの公開鍵証明書によるユーザ１からの指示要求メッセージの正当性の確認をも行う。口座管理サーバ５は、更に、ユーザ１の口座について上記指示要求メッセージに従った処理を実行し、処理を実行した旨の処理完了メッセージを作成してユーザ１に送付する。

【００２０】図２は、図１のオンライン金融取引システムにおいて、ユーザ１が口座管理機関３に対し口座開設要求を送付したときの処理流れを示した図である。

【００２１】この処理流れでは、ユーザ１が口座管理サーバ５に口座開設要求を送付することにより、新規口座の開設要求と共に新規口座開設に伴う必要情報としての個人認証情報の登録要求がユーザ１から口座管理機関３に与えられることになる。そのため上記システムでは、口座開設要求の送付により口座開設に必要な処理動作と共にユーザ１の個人認証情報を登録する処理動作が実行される。

【００２２】まず、ユーザ１は口座管理機関３において自己の口座を新規開設すべく、口座管理サーバ５に対し口座開設要求を送付する。この口座開設要求は、口座種別（例えば、総合／当座の別）等を明示しており、また、口座管理機関３に対するユーザ１の個人認証情報登録要求でもある（ステップＳ１２１）。

【００２３】口座管理機関３では、口座管理サーバ５が

上記要求を受取ると、口座の新規開設に伴って生じる情報（口座情報）１１である口座番号情報や口座種別情報等を、口座管理サーバ５を通してユーザ１に送付する（ステップＳ１２２）。

【００２４】上記口座情報１１を受取ると、ユーザ１は、まずその口座情報１１の内容を確認し、次にその口座情報１１に、ＣＡ（図示しない）から取得した自己の公開鍵証明書を結合させて自己の個人認証情報１３を生成する。更にこの生成した個人認証情報１３に対し、上記公開鍵証明書で証明されている公開鍵に対応する上記個人秘密鍵（ＩＣカード等に秘密に保管されている）により電子署名１５を作成する。この電子署名１５は、例えば口座情報１１や個人認証情報１３等の文書のハッシュ情報を暗号化して文書に添付することにより行われる。そして、このようにして構成したユーザ１の電子署名付き個人認証情報１３を、口座管理サーバ５に送付する。この電子署名付き個人認証情報１３は、第三者が利用したり改竄したりすることができないセキュリティの高い情報である（ステップＳ１２３）。

【００２５】上記電子署名付き個人認証情報１３を受取ると、口座管理サーバ５は、まず受取った上記個人認証情報１３内に含まれる公開鍵証明書を使用してその個人認証情報１３に添付されている電子署名１５の検証を行うことにより、その個人認証情報１３の正当性を確認する。この電子署名１５の検証は、例えば署名部分を公開鍵で復号化した情報と文書のハッシュ情報とが同一であるか否かを確認することによって行う。電子署名１５がユーザ１により自己の公開鍵に対応する個人秘密鍵を用いて作成されたのであるから、個人認証情報１３の正当性は確認できるはずである。正当性の確認が行われた後は、個人認証情報１３を口座開設に伴う個人認証情報として電子署名１５が添付された状態で口座情報管理ＤＢ７に登録する（ステップＳ１２４）。これにより、新規口座の開設が確立されるので、口座管理サーバ５は、ユーザ１の新規口座の開設が確立された旨のメッセージ１７をユーザ１に送付する（ステップＳ１２５）。そして、ユーザ１がそのメッセージ１７を確認すると（ステップＳ１２６）、口座開設要求（個人認証情報登録要求）に関する一連の処理動作が完了する。

【００２６】図３は、図１のオンライン金融取引システムにおいて、ユーザ１が開設済みの自己の口座にアクセスして商取引に利用するときの処理流れを示した図である。

【００２７】図３において、まずユーザ１は、口座管理機関３に開設済みの自己の口座を利用して実行したい取引内容（指示内容）を明記した処理メッセージ１９、例えば「¥5000をxxxxに振替えたい」というような振替依頼等の処理メッセージ１９を作成する（ステップＳ１３１）。

【００２８】次に、この処理メッセージ１９に対して、

口座情報管理ＤＢ７に登録済みの公開鍵証明書で証明されている公開鍵に対応する個人秘密鍵により電子署名１５を作成する（ステップＳ１３２）。そして、口座に対する指示内容である上記処理メッセージ１９に上記電子署名１５を結合させて指示要求メッセージ２１を作成し、これを口座管理サーバ５に送付する（ステップＳ１３３）。

【００２９】上記指示要求メッセージ２１を受取ると、口座管理サーバ５は、ユーザ１の個人認証情報１３として口座情報管理ＤＢ７に登録されている公開鍵証明書中の公開鍵により、上記指示要求メッセージ２１の正当性を検証する。この検証では、例えば上記指示要求メッセージ２１が口座開設者自身からの指示要求であるか否かや、第三者による指示内容の改竄が行われているか否か等が確認される（ステップＳ１３４）。その結果、上記指示要求メッセージ２１の正当性が確認されると、口座管理サーバ５は、ユーザ１の口座に対して上記指示要求メッセージ２１に従った処理（例えば、ユーザ１の口座から他人の口座への振替等）を実行し（ステップＳ１３５）、例えば振替を行った旨の処理完了メッセージ２３を作成してユーザ１に送付する（ステップＳ１３６）。そして、ユーザ１がそのメッセージ２３を確認すると、開設済み口座を商取引に利用するときの一連の処理動作が完了する。

【００３０】以上説明したように、本発明の一実施形態によれば、ユーザ１が予め信頼できるＣＡから個人認証情報として使用するために取得しておいた自己の公開鍵証明書と口座情報１１とを結合させて個人認証情報１３を生成する。そして、公開鍵証明書中の公開鍵に対応する個人秘密鍵により作成した電子署名１５を個人認証情報１３に添付することとした。そのため、ＰＩＮをネットワーク９上に流すことなく、個人認証を行うことができる。また、ユーザ１の電子署名１５により個人認証情報１３の完全性を保証することができるため、口座番号と公開鍵の完全性をユーザ１によって管理することが可能となり、銀行等の口座管理機関３でさえも個人認証情報１３を変更することができない。また、第三者がユーザ本人になりすまして口座情報１１を不正使用したり、口座情報１１の変更を不正に指示したりする危険性もなくなる。更には、ユーザ本人しか持ち得ない秘密鍵のみで自己の口座にアクセスが可能なため、自己の口座に対して行ったアクセスを、ユーザ自身も否認することができなくなる。

【００３１】上述した内容は、あくまで本発明の一実施形態に関するものであって、本発明が上記内容のみに限定されることを意味するものでないのは勿論である。

【００３２】

【発明の効果】以上説明したように、本発明によれば、個人認証情報の漏洩が生じても第三者に利用されたり内容が改竄されたりする虞がなく、且つ、個人情報の管理機関が必要に応じて内容を確認することが可能な個人認証情報の管理方式を提供することができる。

【図面の簡単な説明】

【図１】本発明の個人情報の管理方式が適用されるオンライン金融取引システムの一実施形態を示すブロック図。

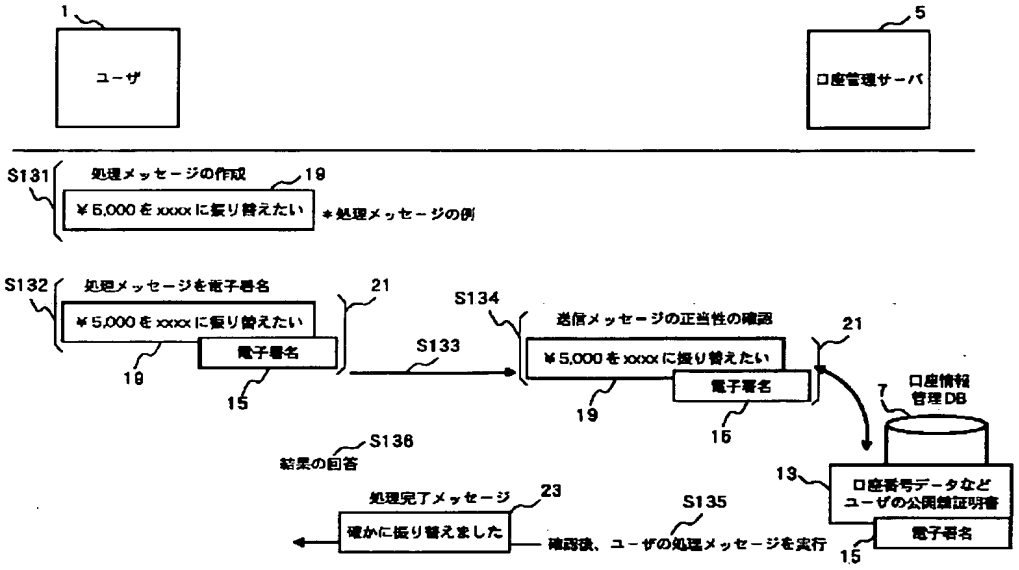
【図２】図１のシステムにおける、口座開設に伴う処理流れを示した図。

【図３】図１のシステムにおける、開設済み口座を商取引に利用するときの処理流れを示した図。

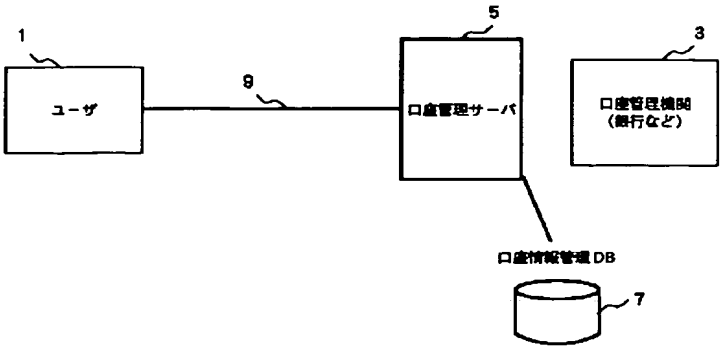
【符号の説明】

１　ユーザ
３　口座管理機関
５　口座管理サーバ
７　口座情報管理データベース（ＤＢ）
９　ネットワーク
１１　口座情報
１３　個人認証情報
１５　電子署名
１７　新規口座開設の確立のメッセージ
１９　処理メッセージ
２１　指示要求メッセージ
２３　処理完了メッセージ

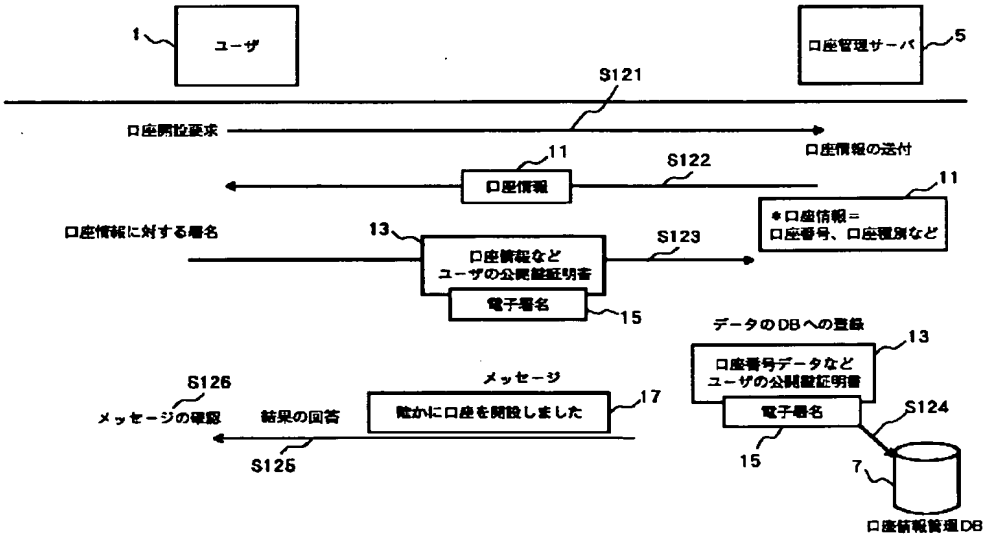
【図３】


1
ユーザ
5
口座管理サーバ
S131
処理メッセージの作成
19
￥5,000 を xxxx に振り替えたい
＊処理メッセージの例
S132
処理メッセージを電子署名
21
￥5,000 を xxxx に振り替えたい
電子署名
19
15
S133
S134
送信メッセージの正当性の確認
￥5,000 を xxxx に振り替えたい
電子署名
19
15
21
7
口座情報
管理DB
13
口座番号データなど
ユーザの公開鍵証明書
電子署名
15
S135
確認後、ユーザの処理メッセージを実行
S136
結果の回答
処理完了メッセージ
23
確かに振り替えました

【図１】


1
ユーザ
9
5
口座管理サーバ
3
口座管理機関
（銀行など）
口座情報管理DB
7

【図２】


1
ユーザ
口座管理サーバ
5
S121
口座開設要求
口座情報の送付
11
口座情報
S122
11
＊口座情報＝
口座番号、口座種別など
口座情報に対する署名
13
口座情報など
ユーザの公開鍵証明書
S123
電子署名
15
データのDBへの登録
13
口座番号データなど
ユーザの公開鍵証明書
電子署名
S124
15
7
口座情報管理DB
S126
メッセージの確認
結果の回答
メッセージ
無かに口座を開設しました
17
S125

JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11)Publication number: 11065443
(43)Date of publication of application: 05.03.1999

(51)Int.Cl.

G09C 1/00
G09C 1/00
G06F 19/00
H04L 9/32

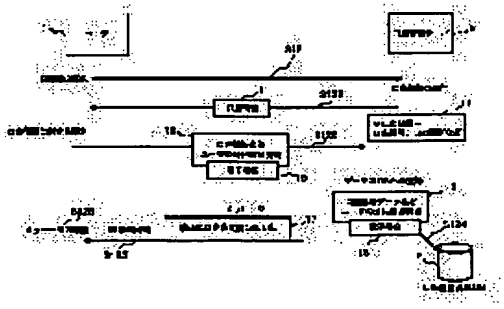
(21)Application number: 09219398
(22)Date of filing: 14.08.1997

(71)Applicant: N T T DATA:KK
(72)Inventor: HATTORI NOBORU
NASU YOSHIYUKI
SAKATA YUJI

(54) MANAGEMENT ELEMENT SYSTEM FOR INDIVIDUAL AUTHENTICATION INFORMATION

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent individual authentication information from being used illegally or altered by a 3rd person and to enable a management organ for individual information to confirm its contents at need.
SOLUTION: A user sends an account opening request specifying an account kind to an account management server 5. The account management server 5 sends account information 11 accompanying the opening of a new account to the user 1. The user 1 confirms the contents of the account information 11 and combines an open key certificate from CA(certification authority) to generate user's own individual authentication information 13. For the individual authentication information 13, an electronic signature 15 is generated with an individual secret key corresponding to the open key of the open key certificate. The individual authentication information 13 with the electronic signature is sent to the account management server 5. The account management server 15 verifies the electronic signature 15 by using the open key certificate in the individual authentication information 13 to confirm the adequacy of the individual authentication information 13. The individual authentication information 13 is registered in an account information management DB 7 while the electronic signature 15 is added. The account management server 5 sends a message indicating the opening of the new account to the user 1, who confirms the message 17, thus completing a series of processing operations regarding the account opening request.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998 Japanese Patent Office

HEI 11-65443

[CLAIMS]

[Claim 1]

Personal authentication information management system for the same information exchanged between users and information management institutions, characterized in comprising a generating means for generating a personal authentication information formed of intrinsic code information of said users and official password information of said users.

[Claim 2]

Personal authentication information management system as claimed in claim 1, characterized in that said generating means is provided in said users.

[Claim 3]

Personal authentication information management system as claimed in claim 1, characterized in that said personal authentication information is exchanged between said users and servers installed in said information management institutions.

[Claim 4]

Personal authentication information system as claimed in claim 1, characterized in that said personal authentication information is exchanged for dealings conducted between said users and said servers.

[Claim 5]

Personal authentication information management

system as claimed in claim 4, characterized in that said dealing is an on-line dealing conducted between said users and said servers.

[Claim 6]

Personal authentication information management system as claimed in claim 1, characterized in that:

said information management institutions are financial institutions; and

said code information is the number information indicating the account number of user registered in said final institution.

[Claim 7]

Personal authentication information management system as claimed in claim 1, characterized in that said official password information has been acquired previously for use as the personal authentication information of a user itself from the certification authority as the third party.

[Claim 8]

Personal authentication information management system as claimed in claim 7, characterized in that a personal secret password information corresponding to said official password information is further used.

[Claim 9]

Personal authentication information management system as claimed in claim 8, characterized in that said personal secret password information is used for

generation of electronic signature to be attached to the personal authentication information of said users.

[Claim 10]

Personal authentication information management system as claimed in any one of claims 1 to 9, characterized in that said users are provided with;

first means for sending account number registration request to said server;

second means for sending an instruction message about the registered account number to said server; and

third means for sending the personal authentication information with said generated electronic signature when said account number registration request or said instruction message is sent.

[Claim 11]

Personal authentication information management system as claimed in any one of claims 3 to 10, characterized in that said server is provided with a verifying means for verifying justice of the personal authentication information with said electronic signature by verifying said attached electronic signature using the official password information included in the personal authentication information transmitted by said third means.

[Claim 12]

Personal authentication information management system as claimed in claim 11, characterized in that said

information management institution is provided with a storing means for registering said personal authentication information with electronic signature which is verified as the justified information by said verifying means.

[Claim 13]

Personal authentication information management system as claimed in any one of claims 3 to 12, characterized in that said server further comprises a verifying means for verifying justice of the instruction message transmitted by said second means depending on the official password information included in said registered personal authentication information and an executing means for executing such instruction content when justice of said instruction or message is verified.

[Claim 14]

Personal authentication information management system as claimed in claim 13, characterized in that said verifying means verifies justice of said instruction message by checking, based on said registered personal authentication information with electronic signature, whether the instruction message from said user is based on the instruction from a user itself who has registered the account number or not and checking whether instruction content is tampered or not by the third party.

[0005]

Therefore it is an object of the present invention to provide a personal authentication information management system in which there is no fear for use by the third party or tampering of content even when the personal authentication information is leaked and it is possible for the personal information management institution to verify the content of personal information as required.

[0006]

[Means for Solving the Problems]

The personal authentication information management system of the present invention relates to management of personal authentication information to be exchanged between users and information management institutions and is provided with a generating means for generating personal authentication information formed of the intrinsic code information of user and official password information of user.

[0007]

In the preferred embodiment of the present invention, the generating means is provided in user side. Personal authentication information is exchanged between a user and a server provided in information management institution. For example, such personal authentication information is exchanged for the dealing performed between a user and a server. As the dealing explained

above, an on-line dealing, for example, is conducted between a user and a server.

[0008]

The information management institution means a financial institution such as a bank or the like. Intrinsic code information of user means the number information indicating the account number of a user registered in a financial institution.

[0009]

The official password information explained above has been previously acquired for use as the personal authentication information of user itself from a certification authority (CA) working as the third party institution. The personal authentication information further includes a personal secret password information corresponding to this official password information. This personal secret password information is used for generation of electronic signature to be attached to the personal authentication information of user.

[0010]

With attachment of such electronic signature, illegal access to the account number of a user by the third party can be prevented and moreover alteration (tampering) of personal authentication information of user in the information management institution can also be prevented.

[0011]

In the embodiment explained above, a user is provided, in addition to the generating means explained above, with a first means for sending an account number registering request to a server, a second means for sending in instruction message about the registered account number to the server and a third means for sending, to the server, the personal authentication information with electronic signature generated when the registration request or instruction message is sent.

[0012]

On the other hand, the server is provided with a verifying means for verifying justice of the personal authentication information with electronic signature by verifying the attached electronic signature using the official password information included in the personal authentication information sent from said third means. The personal authentication information with electronic signature which is verified as the justified information by this verifying means is registered to the memory means provided in the information management institution. The server is also provided, in addition to the first to third means, with a verifying means for verifying justice of instruction message sent by the second means depending on the official password information included in the registered personal authentication information and an executing means for executing such instruction content when justice of instruction message is verified.

[0013]

The verifying means for verifying justice of instruction message verifies justice of instruction message by verifying, based on the registered personal authentication information with electronic signature, whether the instruction message sent from a user is the instruction issued from a user itself who has registered the account number or not and whether instruction content is tampered by the third party or not.

[0014]

The verifying means enables the information management institution to use, as required, the personal authentication information of the user who has registered the account number.